February 18, 2011
Via ECFS

Ms. Marlene H. Dortch, FCC Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

RE: EB Docket No. 06-36
Annual 64.2009(e) CPNI Certification for Calendar Year 2010
Ojo Service LLC 499 Filer ID: 828187

Dear Ms. Dortch:

Attached for filing is the Calendar Year 2010 CPNI Compliance Certification and supporting Statement of CPNI Procedures and Compliance submitted on behalf of Ojo Service LLC. This filing is submitted pursuant to 47 C.F.R. Section 64.2009(e) and in accordance with Public Notice DA 11-159 issued January 28, 2011.

Any questions you may have concerning this filing may be directed to me at 470-740-3031 or via email to sthomas@tminc.com.

Sincerely,

/s/ Sharon Thomas

Sharon Thomas
Consultant to Ojo Service LLC

ST/sp
Attachments
cc: Best Copy and Printing (via email to FCC@BCPIWEB.COM)
C. Vitale – Ojo (via email)
file: Ojo – FCC CPNI
tms: FCC110x CPNI

ANNUAL 47 C.F.R. § 64.2009(e) OFFICER'S CERTIFICATION OF CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE

EB Docket 06-36

Annual 64.2009(e) CPNI Certification:	Covering calendar year 2010
Name of company(s) covered by this certification:	Ojo Service LLC
Form 499 Filer ID:	828187
Name of signatory:	Christopher V. Vitale
Title of signatory:	SVP, General Counsel and Secretary for Worldgate Communications, Inc., sole member of Ojo Service LLC

1. I, Christopher V. Vitale, certify that I am the SVP, General Counsel and Secretary for Worldgate Communications, inc. the sole member of Ojo Service LLC ("Company"), and acting as an agent of Ojo Service LLC, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. §64.2001 *et seq.*

2. Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in §64.2001 *et seq.* of the Commission's rules.

3. The Company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

4. The Company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

5. The Company represents and warrants that the above certification is consistent with 47 C.F.R. §1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Christopher V. Vitale

Christopher V. Vitale, SVP, General Counsel and Secretary of
Worldgate Communications, Inc.,
sole member of Ojo Service LLC

February 18, 2011
Date

Attachments: Accompanying Statement explaining CPNI procedures

Attachment A
Statement of CPNI Procedures and Compliance

Ojo Service LLC

Statement of CPNI Procedures and Compliance

Ojo Service LLC ("Ojo" or "the Company") does not use or permit access to CPNI to market any telecommunications or non-telecommunications services. Ojo has trained its personnel not to use CPNI for marketing purposes. Should Ojo elect to use CPNI in future marketing efforts, it will follow the applicable rules set forth in 47 CFR Subpart U, including, if necessary, the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

Ojo has put into place processes to safeguard its customers' CPNI from improper use or disclosure by employees; and to discover and protect against attempts by third parties to gain unauthorized access to customer CPNI. The Company maintains all CPNI in a secure server environment with limited access and appropriate firewalls and other protections. Internal access to customer information is limited to customer operations and call center employees. The Company has a training process in place for its employees and call center employees regarding the requirements to safeguard CPNI against unauthorized disclosure and has a disciplinary process which includes discipline up to and including termination. All employees are required to sign a confidentiality agreement in which they agree to abide by the requirements to maintain confidentiality of customer information in accordance with the CPNI rules and Company policy. The Company's network provider and OSS/BSS provider has similar restrictions regarding customer information in place and are required to maintain those restrictions pursuant to the Company's master services agreement with them.

Ojo does not disclose CPNI to any agents, affiliates, joint venture partners or independent contractors, nor does it use CPNI to identify or track customers who call competing providers. The Company has a strict policy prohibiting the disclosure of CPNI to any third parties, unless required to do so by law (e.g., in response to a subpoena).

Ojo maintains a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI.

The Company does provide call detail information over the telephone subject to the following procedures: Ojo requires a customer to answer a security question (not involving readily available biographical information or account information) when they sign up for service. This question and the answer to the question are visible to only call center representatives and a small number of operational administrative people who have their permissions set to allow them to see this. When a customer calls the call center to discuss their account they have to be able to answer the security question that Ojo asks. If they cannot answer the question Ojo does not provide any information about their account to the calling party. Furthermore, customers have to establish a separate username and password for access to a self-service portal that contains calling detail. If they forget their user name and password Ojo would only reset it for them if they could answer the security question as described above.

The Company allows customers to obtain their call detail information on-line, subject to the following procedures: The customer must create his/her username and password at the time of sale if they want to enter into the customer accessible portal. The customer must then input the

correct username and password for online access. If the customer forgets his/her username and/or password, the Company will reset the password if the Customer is able to answer the security question that was set up when the account was created.

Ojo does not have any retail locations and therefore does not disclose CPNI in-store.

If a customer's account information is changed, the Company immediately notifies the customer of the change via e-mail to the e-mail address of record, without revealing the changed information.

The Company has procedures in place to notify law enforcement in the event of a breach of customers' CPNI and to ensure that the affected customers are not notified of the breach before the time period set forth in the FCC's rules, or, if applicable, when so authorized by law enforcement. Specifically, as soon as practicable, and in no case later than seven business days upon learning of a breach, the Company will notify the U.S. Secret Service and the FBI by electronic means, as required by FCC regulations. The Company will not notify customers or disclose a breach to the public until seven full business days have passed after notification to the U.S. Secret Service and the FBI, unless it believes there is an extraordinarily urgent need to notify customers before seven days in order to avoid immediate and irreparable harm. In that instance, it will only notify such customers *after* consultation with the relevant investigating agency and will cooperate with the agency's request to minimize any adverse effects of the customer notification. If the Company receives no response from law enforcement after the seventh full business day, it will promptly proceed to inform the customers whose CPNI was disclosed of the breach. The Company will delay notification to customers or the public if requested to do so by the U.S. Secret Service or FBI. Notifications to law enforcement and customers are handled by a designated supervisor level employee responsible for managing the company's CPNI compliance.

Ojo has not taken any actions against data brokers in the last year.

Ojo did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2010.

Company has not developed any information with respect to the processes pretexters are using to attempt to access CPNI. If the Company suspects that a pre-texter may be attempting to gain access to CPNI, it will immediately ask the requester to provide information that only the customer would be able to provide and would further investigate suspected pre-texting activity.